A remark on the paper "Randomizing quantum states: Constructions and applications"

Guillaume Aubrun

A REMARK ON THE PAPER "RANDOMIZING QUANTUM STATES: CONSTRUCTIONS AND APPLICATIONS"

GUILLAUME AUBRUN

Abstract. The concept of ε-randomizing quantum channels has been introduced by Hayden, Leung, Shor and Winter in connection with approximately encrypting quantum states. They proved using a discretization argument that sets of roughly $d \log d$ random unitary operators provide examples of such channels on $\mathbf{C}^d$. We show that a simple trick improves the efficiency of the argument and reduces the number of unitary operators to roughly d.

Since our argument is a minor modification of the original proof, we systematically refer the reader to [1] for introduction, background and applications of the notion of randomizing states.

Notation. On the space $\mathcal{B}(\mathbf{C}^d)$ of $d \times d$ complex matrices we consider the trace class norm $\|\cdot\|_1$ and the operator norm $\|\cdot\|_\infty$. Let also $\mathcal{D}(\mathbf{C}^d)$ be the convex set of mixed states (=positive elements of $\mathcal{B}(\mathbf{C}^d)$ with trace 1). The extreme points of $\mathcal{D}(\mathbf{C}^d)$ are pure states. We denote by C and c absolute numeric constants.

Definition. *A quantum channel (= completely positive trace-preserving linear map) $R : \mathcal{B}(\mathbf{C}^d) \to \mathcal{B}(\mathbf{C}^d)$ is said to be ε-randomizing if for every state $\varphi \in \mathcal{D}(\mathbf{C}^d)$,*

$$\left\| R(\varphi) - \frac{\mathrm{Id}}{d} \right\|_\infty \leqslant \frac{\varepsilon}{d}.$$

Theorem. *Let $(U_i)_{1 \leqslant i \leqslant N}$ be independent random matrices Haar-distributed on the unitary group $\mathcal{U}(d)$. Let $R : \mathbf{C}^d \to \mathbf{C}^d$ be the quantum channel defined by*

$$R(\varphi) = \frac{1}{N} \sum_{i=1}^{N} U_i \varphi U_i^\dagger.$$

Assume that $0 < \varepsilon < 1$ and $N \geqslant Cd/\varepsilon^2 \cdot \log(1/\varepsilon)$. Then the channel R is ε-randomizing with nonzero probability.

As often with random constructions, we actually prove that the conclusion holds true with *large* probability. Let us quote two lemmas from [1].

Lemma (Lemma II.3 in [1])**.** *Let φ, ψ be pure states on $\mathbf{C}^d$ and $(U_i)_{1 \leqslant i \leqslant N}$ as before. Then for every $0 < \delta < 1$,*

$$\mathbf{P}\left(\left| \frac{1}{N} \sum_{i=1}^{N} \mathrm{Tr}(U_i \varphi U_i^\dagger \psi) - \frac{1}{d} \right| \geqslant \frac{\delta}{d} \right) \leqslant 2 \exp(-c\delta^2 N)$$

Lemma (Lemma II.4 in [1])**.** *For $0 < \delta < 1$ there exists a set $\mathcal{M}$ of pure states on $\mathbf{C}^d$ with $|\mathcal{M}| \leqslant (5/\delta)^{2d}$, such that for every pure state φ on $\mathbf{C}^d$, there exists $\varphi_0 \in \mathcal{M}$ such that $\|\varphi - \varphi_0\|_1 \leqslant \delta$.*

Proof of the theorem. Let A be the (random) quantity

$$A = \sup_{\varphi,\psi\in\mathcal{D}(\mathbf{C}^d)} \left| \frac{1}{n}\sum_{i=1}^n \mathrm{Tr}(U_i\varphi U_i^\dagger\psi) - \frac{1}{d}\right|.$$

We must show that $\mathbf{P}(A \geqslant \frac{\varepsilon}{d}) < 1$. Let B be the restricted supremum over the set $\mathcal{M}$

$$B = \sup_{\varphi_0,\psi_0\in\mathcal{M}} \left| \frac{1}{n}\sum_{i=1}^n \mathrm{Tr}(U_i\varphi_0 U_i^\dagger\psi_0) - \frac{1}{d}\right|.$$

It follows from the lemmas that for δ to be determined later

$$\mathbf{P}\left(B \geqslant \frac{\delta}{d}\right) \leqslant (5/\delta)^{4d}\cdot 2\exp(-c\delta^2 N).$$

Note that for any self-adjoint operators $a, b \in \mathcal{B}(\mathbf{C}^d)$

$$\left| \frac{1}{n}\sum_{i=1}^n \mathrm{Tr}(U_i a U_i^\dagger b)\right| \leqslant \|a\|_1\|b\|_1\left(A + \frac{1}{d}\right). \tag{1}$$

By a convexity argument, the supremum in A can be restricted to pure states. Let φ, ψ be pure states and φ_0, ψ_0 in $\mathcal{M}$ so that $\|\varphi - \varphi_0\|_1 \leqslant \delta, \|\psi - \psi_0\|_1 \leqslant \delta$. Then

$$\begin{aligned}\left| \frac{1}{n}\sum_{i=1}^n \mathrm{Tr}(U_i\varphi U_i^\dagger\psi) - \frac{1}{d}\right| \quad &\leqslant \quad \left| \frac{1}{n}\sum_{i=1}^n \mathrm{Tr}(U_i\varphi_0 U_i^\dagger\psi_0) - \frac{1}{d}\right| \\ &\quad + \left| \frac{1}{n}\sum_{i=1}^n \mathrm{Tr}(U_i(\varphi-\varphi_0) U_i^\dagger\psi_0)\right| + \left| \frac{1}{n}\sum_{i=1}^n \mathrm{Tr}(U_i\varphi U_i^\dagger(\psi-\psi_0))\right|.\end{aligned}$$

Taking the supremum over φ, ψ and using twice (1), we get $A \leqslant B + 2\delta(A + 1/d)$, and so

$$A \leqslant \frac{1}{1-2\delta}\left(B + \frac{2\delta}{d}\right).$$

Choosing $\delta = \varepsilon/(3+2\varepsilon) \geqslant \varepsilon/5$ gives

$$\mathbf{P}\left(A \geqslant \frac{\varepsilon}{d}\right) \leqslant \mathbf{P}\left(B \geqslant \frac{\delta}{d}\right) \leqslant 2\left(\frac{25}{\varepsilon}\right)^{4d}\exp(-c\varepsilon^2 N/25).$$

The last quantity is less than 1 provided $N \geqslant Cd/\varepsilon^2 \cdot \log(1/\varepsilon)$ for some constant C.

Remark. *One checks (using the value $c = (6\ln 2)^{-1}$ from [1]) that for d large enough, the constant in our theorem can the chosen to $C = 150$. This is presumably far from optimal.*

References

[1] P. Hayden, D. Leung, P. W. Shor and A. Winter, Randomizing quantum states: constructions and applications, *Comm. Math. Phys.* **250** (2004), 371–391.

Address : Université de Lyon, Université de Lyon 1,
CNRS, UMR 5208 Institut Camille Jordan,
Batiment du Doyen Jean Braconnier,
43, boulevard du 11 novembre 1918,
F - 69622 Villeurbanne Cedex, France.

e-mail: aubrun@math.univ-lyon1.fr